IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant(s)	: D. ANDREEV et al.	Confirmation No.: 1826
Appln. No.	: 10/791,322	Group Art Unit: 2139
Filed	: March 2, 2004	Examiner: A. F. Tabor
For	: SYSTEM AND METHOD OF PROVIDING CREDENTIALS IN A NETWORK	

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Commissioner for Patents
U.S. Patent and Trademark Office
Customer Window, Mail Stop Appeal Brief-Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

This appeal is from the Examiner's final rejection of claims 1, 3-10, 13-19 and 21-25 as set forth in the Final Office Action of July 22, 2008. A Notice of Appeal, in response to the July 22, 2008 Final Office Action, was filed on October 20, 2008. The instant Appeal Brief is being timely filed within two months of the Notice of Appeal.

Payment in the amount of $ 540.00 is being concurrently submitted as payment of the requisite fee under 37 C.F.R. 41.20(b)(2). No additional fee is believed to be required for filing the instant Appeal Brief. However, if for any reason a necessary fee is required for consideration of the instant paper, authorization is hereby given to charge the fee for the Appeal Brief and any necessary extension of time fees to Deposit Account No. 09-0457.

TABLE OF CONTENTS

(I) REAL PARTY IN INTEREST

The real party in interest is International Business Machines Corporation by an assignment recorded in the U.S. Patent and Trademark Office on April 14, 2004, at Reel 014517 and Frame 0546.

(II) RELATED APPEALS AND INTERFERENCES

No related appeals and/or interferences are pending.

(III) STATUS OF THE CLAIMS

Claims 1, 3-10, 13-19 and 21-25 are the only pending claims. Claims 2, 11, 12 and 20 are canceled. Claims 1, 3-10, 13-19 and 21-25 stand finally rejected. Claims 1, 3-10, 13-19 and 21-25 are the subject of this appeal. The claims in issue are attached in the "Claims Appendix".

(IV) STATUS OF THE AMENDMENTS

A Response under 37 C.F.R.§ 1.116 was filed September 15, 2008, requesting reconsideration of the finally rejected claims. The Examiner responded with an Advisory Action mailed September 24, 2008, indicating that the Response was considered but did not place the application in condition for allowance. Appellants submit that no other amendments after final have been filed; however, all amendments to the claims have been entered.

(V) SUMMARY OF THE CLAIMED SUBJECT MATTER

A. The Claimed Subject Matter

1. INDEPENDENT CLAIM 1

With reference to pages 5-13 of the instant application and to the figures, and by way of non-limiting example, the invention provides for a method for authentication in a network wherein the method comprises creating a credential string on a portal server (110) wherein the credential string is an encrypted hash of a session ID (see page 7, lines 12-14, page 9, lines 1-4, page 11, line 10, and page 12, lines 7-8 of the instant specification). The method also includes sending a UserID associated with the session ID and the credential string to a software application from the portal server (110), while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server (see page 9, lines 1-9, page 11, lines 10-14, page 5, lines 12-13, and page 7, lines 4-8 of the instant specification). The method additionally includes receiving a confirmation request from the software application to an LDAP proxy (115) while maintaining the user password on the portal server (110) such that the user password is not required to authenticate the User ID, wherein the confirmation request includes the credential string (see page 12, lines 15-21, page 7, lines 4-8, and page 8, lines 13-14 of the instant specification). Furthermore, the method includes sending a response from the LDAP proxy (115) in reply to the confirmation request to validate the credential string to authenticate the UserID (see page 7, line 18 to page 8, line 4, page 9, lines 14-19, and page 12, line 20 to page 13, line 2 of the instant specification).

2. INDEPENDENT CLAIM 9

With reference to pages 5-13 of the instant application and to the figures, and by way of non-limiting example, the invention provides for a method for authenticating a user request for a software application, wherein the method comprises receiving a UserID and a credential string at an authentication proxy server (115) (see page 7, lines 9-17 and page 9, lines 1-4 of the specification), wherein the credential string is an encrypted hash of a session ID (see page 7, lines 4-9 of the specification), which is created at a portal (110) (see page 7, lines 9-12 and page 11, line 10 of the specification). The method also comprises sending a confirmation request from the authentication proxy (115) to the portal (110) while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal, wherein the confirmation request includes the credential string (see page 11, lines 11-14, page 12, lines 15-21, page 7, lines 4-8 and page 8, lines 13-14 of the specification). The method additionally includes receiving a response at the authentication proxy (115) for the confirmation request while maintaining the user password on the portal (110) such that the user password is not required to authenticate the User ID (see page 12, lines 15-21, page 7, lines 4-8 and page 8, lines 13-14 of the specification). Furthermore, the method includes validating the UserID using a light weight directory access protocol (LDAP) lookup request and the response (see page 9, lines 11-19 and page 11, lines 14-15 of the specification).

3. INDEPENDENT CLAIM 15

With reference to pages 5-13 of the instant application and to the figures, and by way of non-limiting example, the invention provides for a system for authenticating a session stored on a computer readable storage medium, wherein the system comprises a computer readable program code, comprising an authentication proxy (115) which receives requests to authenticate a UserID and a credential string, the credential string being an encrypted hash of a session ID and created on a portal (110) (see page 7, lines 4-17, page 9, lines 1-4 and page 11, line 10 of the specification). The system also includes a credential string validation component (112) which receives requests to validate the credential string while maintaining a user password on the portal such that the user password is not required to validate the credential string (see page 7, lines 4-8, page 7, line 18 to page 8, line 4, page 8, lines 13-14, page 9, lines 14-19, and page 12, line 15 to page 13, line 2 of the specification). The credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal (see page 5, lines 12-13, page 7, line 18 to page 8, line 14, and page 9, lines 1-4 of the specification).

4. INDEPENDENT CLAIM 22

With reference to pages 5-13 of the instant application and to the figures, and by way of non-limiting example, the invention provides for a computer program product comprising a computer usable medium having readable program code embodied in the medium, wherein the computer program product includes at least one program code to create a credential string on a portal server (110), wherein the credential string is an encrypted hash of a session ID (see page 7, lines 12-14, page 9, lines 1-4, page 11, line 10, and page 12, lines 7-8 of the instant specification). The at least one program code also sends a UserID associated with the session ID and the credential string to a software application from the portal server (110), while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server (see page 9, lines 1-9, page 11, lines 10-14, page 5, lines 12-13, and page 7, lines 4-8 of the instant specification). The at least one program code additionally receives a confirmation request from the software application to an LDAP proxy (115) while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, wherein the confirmation request includes the credential string (see page 12, lines 15-21, page 7, lines 4-8, and page 8, lines 13-14 of the instant specification). Furthermore, the at least one program code sends a response from the LDAP proxy (115) in reply to the confirmation request to validate the credential string to authenticate the UserID (see page 7, line 18 to page 8, line 4, page 9, lines 14-19, and page 12, line 20 to page 13, line 2 of the instant specification).

(VI) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 3-5, 8-10, 13, 14 and 22 are improperly rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 6,539,482 to BLANCO et al.

Whether claims 6, 7, 15, 19 and 23-25 are improperly rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 7,100,054 to WENISCH et al.

Whether claims 16-18 and 21 are improperly rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and U.S. Patent No. 7,100,054 to WENISCH et al., and further in view of U.S. Patent No. 6,539,482 to BLANCO et al.

(VII) ARGUMENT RE. 103(a) REJECTIONS

(A) The rejection of 1, 3-5, 8-10, 13, 14 and 22 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 6,539,482 to BLANCO et al. is improper and should be withdrawn.

REJECTION OF INDEPENDENT CLAIM 1 UNDER 35 U.S.C. § 103 IS IN ERROR

The rejection of claim 1 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 6,539,482 to BLANCO et al. is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

Claim 1 recites, in pertinent part:

> ... creating a credential string on a portal server, the credential string being an encrypted hash of a session ID;

> sending a UserID associated with the session ID and the credential string to a software application from the portal server, while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server;
>
> receiving a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, the confirmation request including the credential string…

Appellant agrees with the Examiner (see page 3 of the Final Office Action) that YOUNG fails to teach maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal. However, Appellant disagrees that KAUFMAN teaches or suggests these features.

It is not disputed that KAUFMAN teaches to create two separate hash values (H1 and H2) of the user's password (P) wherein the hash values of the password are created on a user workstation 12. (See Figs. 4 and 5; Col. 6, lines 42-44.) KAUFMAN uses the login agent's public key (LA-PUB) to encrypt H2 along with a randomly generated secret nonce key K. KAUFMAN combines the user name N with encrypted H2 and K to create a message M. This message, which includes a hashed version of the password H2, is sent to the login agent 26. (Col. 7, lines 25-44; Figs. 4 and 5.) The login agent parses out the username N and sends it to a certificate storage server (CSS) 24. The CSS uses the username N to find the user's encrypted credentials {U}H1, which is an encryption of H1 and the user's private RSA key U. KAUFMAN appends the encrypted credential {U}H1 to H2 and encrypts the combination using the login agent's public key (LA-PUB) to form a doubly encrypted credential D. (Col. 6, lines 51-60.) This doubly encrypted credential D, which contains hashed passwords H1 and H2, is sent to the

login agent 26. (Col. 7, lines 44-56; See Fig. 3).

As such, it is apparent that KAUFMAN uses a variety of hashing and encryption mechanisms to protect the user's password before the password is sent from the user's workstation to a login agent, from the login agent to a CSS, and from the CSS back to the login agent, etc. However, despite these hashing and encryption mechanisms, KAUFMAN still exposes the user's password to a variety of network resources. As such, Appellant submits that contrary to the Examiner's assertions, KAUFMAN does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

In the Advisory Action, the Examiner points to the Abstract and col. 4, lines 59-60 of KAUFMAN as teaching to maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. Appellant disagrees. While it is true that the Abstract states that the logon agent is not trusted with the user's password, this is not the same as maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal. Furthermore, while it is true that the language of col. 4, lines 59-60 of KAUFMAN states that the user's private RSA key is not revealed to any other party, this is not the same as maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal. A private RSA key is not a password.

BLANCO does not cure the deficiencies of YOUNG and KAUFMAN. In particular, Appellant submits that BLANCO does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. While it is apparent that BLANCO teaches an authentication system which includes a directory service containing a

remote access password and a standard access password for each user of the network, BLANCO uses an authentication protocol that provides information on whether a user is accessing the network locally or remotely, and includes a front-end between the directory service and the authentication protocol. The front-end receives a user identifier and a user password entered by a user through the authentication protocol, and retrieves from the directory service the remote access password and the standard access password corresponding to the user identifier. If the authentication protocol indicates a remote access, the front-end compares the user password to the remote access password, else it compares the user password to the standard access password. Access to the network is granted if the comparison is successful. (Abstract; See, e.g., Fig. 2). As such, BLANCO does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

Because the above-noted documents fail to disclose or suggest, at least the above-noted features of the instant invention, Appellant submits that no proper combination of these documents renders unpatentable the combination of features recited in at least independent claim 1.

REJECTION OF INDEPENDENT CLAIM 9 UNDER 35 U.S.C. § 103 IS IN ERROR

The rejection of claim 9 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 6,539,482 to BLANCO et al. is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

Claim 9 recites, in pertinent part:

> ... receiving a UserID and a credential string at an authentication proxy server, the credential string being an encrypted hash of a session ID, which is created at a portal;
>
> sending a confirmation request from the authentication proxy to the portal while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal, the confirmation request includes the credential string;
>
> receiving a response at the authentication proxy for the confirmation request while maintaining the user password on the portal such that the user password is not required to authenticate the User ID...

Appellant agrees with the Examiner (see page 4 of the Final Office Action) that YOUNG fails to teach maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal. However, Appellant disagrees that KAUFMAN teaches or suggests these features.

It is not disputed that KAUFMAN teaches to create two separate hash values (H1 and H2) of the user's password (P) wherein the hash values of the password are created on a user workstation 12. (See Figs. 4 and 5; Col. 6, lines 42-44.) KAUFMAN uses the login agent's public key (LA-PUB) to encrypt H2 along with a randomly generated secret nonce key K. KAUFMAN combines the user name N with encrypted H2 and K to create a message M. This message, which includes a hashed version of the password H2, is sent to the login agent 26. (Col. 7, lines 25-44; Figs. 4 and 5.) The login agent parses out the username N and sends it to a certificate storage server (CSS) 24. The CSS uses the username N to find the user's encrypted credentials {U}H1, which is an encryption of H1 and the user's private RSA key U. KAUFMAN appends the encrypted credential {U}H1 to H2 and encrypts the combination using the login

agent's public key (LA-PUB) to form a doubly encrypted credential D. (Col. 6, lines 51-60.) This doubly encrypted credential D, which contains hashed passwords H1 and H2, is sent to the login agent 26. (Col. 7, lines 44-56; See Fig. 3).

As such, it is apparent that KAUFMAN uses a variety of hashing and encryption mechanisms to protect the user's password before the password is sent from the user's workstation to a login agent, from the login agent to a CSS, and from the CSS back to the login agent, etc. However, despite these hashing and encryption mechanisms, KAUFMAN still exposes the user's password to a variety of network resources. As such, Appellant submits that contrary to the Examiner's assertions, KAUFMAN does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

In the Advisory Action, the Examiner points to the Abstract and col. 4, lines 59-60 of KAUFMAN as teaching to maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. Appellant disagrees. While it is true that the Abstract states that the logon agent is not trusted with the user's password, this is not the same as maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal. Furthermore, while it is true that the language of col. 4, lines 59-60 of KAUFMAN states that the user's private RSA key is not revealed to any other party, this is not the same as maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal. A private RSA key is not a password.

BLANCO does not cure the deficiencies of YOUNG and KAUFMAN. In particular, Appellant submits that BLANCO does not maintain the user password on the portal and avoid

exposing the user password to network resources beyond the portal. While it is apparent that BLANCO teaches an authentication system which includes a directory service containing a remote access password and a standard access password for each user of the network, BLANCO uses an authentication protocol that provides information on whether a user is accessing the network locally or remotely, and includes a front-end between the directory service and the authentication protocol. The front-end receives a user identifier and a user password entered by a user through the authentication protocol, and retrieves from the directory service the remote access password and the standard access password corresponding to the user identifier. If the authentication protocol indicates a remote access, the front-end compares the user password to the remote access password, else it compares the user password to the standard access password. Access to the network is granted if the comparison is successful. (Abstract; See, e.g., Fig. 2). As such, BLANCO does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

Because the above-noted documents fail to disclose or suggest, at least the above-noted features of the instant invention, Appellant submits that no proper combination of these documents renders unpatentable the combination of features recited in at least independent claim 9.

REJECTION OF INDEPENDENT CLAIM 22 UNDER 35 U.S.C. § 103 IS IN ERROR

The rejection of claim 22 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 6,539,482 to BLANCO et al. is in error, the decision of

the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

Claim 22 recites, in pertinent part:

> ... create a credential string on a portal server, the credential string being an encrypted hash of a session ID;
>
> send a UserID associated with the session ID and the credential string to a software application from the portal server, while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server;
>
> receive a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, the confirmation request including the credential string...

Appellant agrees with the Examiner (see page 5 of the Final Office Action) that YOUNG fails to teach maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal. However, Appellant disagrees that KAUFMAN teaches or suggests these features.

It is not disputed that KAUFMAN teaches to create two separate hash values (H1 and H2) of the user's password (P) wherein the hash values of the password are created on a user workstation 12. (See Figs. 4 and 5; Col. 6, lines 42-44.) KAUFMAN uses the login agent's public key (LA-PUB) to encrypt H2 along with a randomly generated secret nonce key K. KAUFMAN combines the user name N with encrypted H2 and K to create a message M. This message, which includes a hashed version of the password H2, is sent to the login agent 26. (Col. 7, lines 25-44; Figs. 4 and 5.) The login agent parses out the username N and sends it to a certificate storage server (CSS) 24. The CSS uses the username N to find the user's encrypted

credentials {U}H1, which is an encryption of H1 and the user's private RSA key U. KAUFMAN appends the encrypted credential {U}H1 to H2 and encrypts the combination using the login agent's public key (LA-PUB) to form a doubly encrypted credential D. (Col. 6, lines 51-60.) This doubly encrypted credential D, which contains hashed passwords H1 and H2, is sent to the login agent 26. (Col. 7, lines 44-56; See Fig. 3).

As such, it is apparent that KAUFMAN uses a variety of hashing and encryption mechanisms to protect the user's password before the password is sent from the user's workstation to a login agent, from the login agent to a CSS, and from the CSS back to the login agent, etc. However, despite these hashing and encryption mechanisms, KAUFMAN still exposes the user's password to a variety of network resources. As such, Appellant submits that contrary to the Examiner's assertions, KAUFMAN does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

In the Advisory Action, the Examiner points to the Abstract and col. 4, lines 59-60 of KAUFMAN as teaching to maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. Appellant disagrees. While it is true that the Abstract states that the logon agent is not trusted with the user's password, this is not the same as maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal. Furthermore, while it is true that the language of col. 4, lines 59-60 of KAUFMAN states that the user's private RSA key is not revealed to any other party, this is not the same as maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal. A private RSA key is not a password.

BLANCO does not cure the deficiencies of YOUNG and KAUFMAN. In particular, Appellant submits that BLANCO does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. While it is apparent that BLANCO teaches an authentication system which includes a directory service containing a remote access password and a standard access password for each user of the network, BLANCO uses an authentication protocol that provides information on whether a user is accessing the network locally or remotely, and includes a front-end between the directory service and the authentication protocol. The front-end receives a user identifier and a user password entered by a user through the authentication protocol, and retrieves from the directory service the remote access password and the standard access password corresponding to the user identifier. If the authentication protocol indicates a remote access, the front-end compares the user password to the remote access password, else it compares the user password to the standard access password. Access to the network is granted if the comparison is successful. (Abstract; See, e.g., Fig. 2). As such, BLANCO does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

Because the above-noted documents fail to disclose or suggest, at least the above-noted features of the instant invention, Appellant submits that no proper combination of these documents renders unpatentable the combination of features recited in at least independent claim 22.

REJECTION OF DEPENDENT CLAIM 3 UNDER 35 U.S.C. § 103 IS IN ERROR

The rejection of claim 3 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent

No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 6,539,482 to BLANCO et al. is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

On page 5 of the Final Office Action, the Examiner cites Fig. 3 of YOUNG and the Abstract of KAUFMAN as teaching wherein the encrypted hash of the session ID is a derivate of the session ID (claim 3). Appellant disagrees.

Fig. 3 of YOUNG shows a method flow diagram with plural text boxes. However, none of the text boxes contains any language with regard to the encrypted hash of the session ID is a derivate of the session ID.

With regard to KAUFMAN, while it is true that the Abstract states that the logon agent is not trusted with the user's password, this is not the same as the encrypted hash of the session ID being a derivate of the session ID.

Because the combination of the above-noted documents fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper combination of these documents renders unpatentable the combination of features recited in at least dependent claim 3.

REJECTION OF DEPENDENT CLAIM 4 UNDER 35 U.S.C. § 103 IS IN ERROR

The rejection of claim 4 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 6,539,482 to BLANCO et al. is in error, the decision of the

Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

On page 5 of the Final Office Action, the Examiner cites Figs. 2 and 3 of BLANCO as teaching performing a lightweight directory access protocol (LDAP) lookup using the UserID and if the LDAP lookup confirms the UserID and the response validates the credential string, returning a successful authentication reply to the software application for establishing a session associated with the session ID, otherwise sending an unsuccessful authentication reply to the software application (claim 4). Appellant disagrees.

Although the language discussing reference 112 in BLANCO discusses granting access and although Fig. 2 shows an LDAP server 24, BLANCO has not been shown to specifically disclose or suggest performing a lightweight directory access protocol (LDAP) lookup using the UserID and if the LDAP lookup confirms the UserID and the response validates the credential string, returning a successful authentication reply to the software application for establishing a session associated with the session ID, otherwise sending an unsuccessful authentication reply to the software application.

Because the combination of the above-noted documents fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper combination of these documents renders unpatentable the combination of features recited in at least dependent claim 4.

REJECTION OF DEPENDENT CLAIM 5 UNDER 35 U.S.C. § 103 IS IN ERROR

The rejection of claim 5 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent

No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 6,539,482 to BLANCO et al. is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

On pages 5-6 of the Final Office Action, the Examiner cites Figs. 3-5 and the Abstract of KAUFMAN as teaching the sending of a UserID and the credential string avoids at least one of sending a user's password outside of a portal server and storing the password in persistent memory (claim 5). Appellant disagrees.

Although Figs. 3-5 of KAUFMAN show a system using credentials, certifications and public and private keys, Fig. 3-5 have not been shown to specifically disclose or suggest sending of a UserID and the credential string avoids at least one of sending a user's password outside of a portal server and storing the password in persistent memory. Furthermore, while it is true that the Abstract states that the logon agent is not trusted with the user's password, this is not the same as sending of a UserID and the credential string avoids at least one of sending a user's password outside of a portal server and storing the password in persistent memory.

Because the combination of the above-noted documents fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper combination of these documents renders unpatentable the combination of features recited in at least dependent claim 5.

REJECTION OF DEPENDENT CLAIM 13 UNDER 35 U.S.C. § 103 IS IN ERROR

The rejection of claim 13 under 35 U.S.C. § 103(a) as being unpatentable over U.S.

Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 6,539,482 to BLANCO et al. is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

On page 6 of the Final Office Action, the Examiner cites Figs. 2 and 3 of BLANCO as teaching validating the confirmation request by assuring that the credential string has been received only once for confirmation at the portal, otherwise, if presented more than once, performing at least one of initiating a security breach procedure and notifying a software application proxy (claim 13). Appellant disagrees.

Although the language discussing reference 112 in BLANCO discusses granting access and although Fig. 2 shows an LDAP server 24, BLANCO has not been shown to specifically disclose or suggest validating the confirmation request by assuring that the credential string has been received only once for confirmation at the portal, otherwise, if presented more than once, performing at least one of initiating a security breach procedure and notifying a software application proxy.

Because the combination of the above-noted documents fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper combination of these documents renders unpatentable the combination of features recited in at least dependent claim 13.

REJECTION OF DEPENDENT CLAIMS 8, 10 AND 14 UNDER 35 U.S.C. § 103 IS IN ERROR

Claims 8, 10 and 14 are dependent claims, depending from distinguishable independent

claims. For these reasons, Appellant submits that these claims are allowable for at least the reasons discussed above with respect to the independent claims.

(B) The rejection of 6, 7, 15, 19 and 23-25 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 7,100,054 to WENISCH et al. is improper and should be withdrawn.

REJECTION OF INDEPENDENT CLAIM 15 UNDER 35 U.S.C. § 103 IS IN ERROR

The rejection of claim 15 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and further in view of U.S. Patent No. 7,100,054 to WENISCH et al. is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

Claim 15 recites, in pertinent part:

> ... wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal.

On page 7 of the Final Office Action, the Examiner acknowledges that YOUNG fails to disclose or suggest maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal. However, Appellant disagrees that these features are taught in either KAUFMAN or WENISCH.

It is not disputed that KAUFMAN teaches using a variety of hashing and encryption mechanisms to protect the user's password before the password is sent from the user's workstation to a login agent, from the login agent to a CSS, and from the CSS back to the login

agent, etc. However, despite these hashing and encryption mechanisms, KAUFMAN nevertheless exposes the user's password to a variety of network resources. As such, Appellant submits KAUFMAN does not teach to maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

WENISCH does not cure the deficiencies of YOUNG and KAUFMAN. In particular, WENISCH also does not teach to maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal. Instead, WENISCH teaches to allow a user to log into a computer. Information from the login, including the user's password and username, are sent to a web server via a login packet. The web server encrypts the password and username and sends it to an authentication provider. (See Fig. 2; Col. 3, line15 – Col. 4, line 35.) As such, WENISCH specifically teaches to send a password from a computer to a web server and to an authentication provider, which teaches away from the claimed invention. However, this is not the same as maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal.

Because the combination of the above-noted documents fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper combination of these documents renders unpatentable the combination of features recited in at least independent claim 15.

REJECTION OF DEPENDENT CLAIMS 6, 7, 19 AND 23-25 UNDER 35 U.S.C. § 103 IS IN ERROR

Claims 6, 7, 19 and 23-25 are dependent claims, depending from distinguishable independent claims. For these reasons, Appellant submits that these claims are allowable for at

least the reasons discussed above with respect to the independent claims.

(C) The rejection of 16-18 and 21 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,024,690 to YOUNG et al. in view of U.S. Patent No. 5,497,421 to KAUFMAN et al. and U.S. Patent No. 7,100,054 to WENISCH et al. and further in view of U.S. Patent No. 6,539,482 to BLANCO et al. is improper and should be withdrawn.

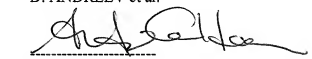
REJECTION OF DEPENDENT CLAIMS 16-18 AND 21 UNDER 35 U.S.C. § 103 IS IN ERROR

Claims 16-18 and 21 are dependent claims, depending from a distinguishable independent claim. For these reasons, Appellant submits that these claims are allowable for at least the reasons discussed above with respect to the independent claims.

CONCLUSION

Each of claims 1, 3-10, 13-19 and 21-25 are patentable under 35 U.S.C. §103(a). Specifically, the applied art of record, even in properly modified, fails to disclose or suggest the unique combination of features recited in Appellant's claims 1, 3-10, 13-19 and 21-25. Accordingly, Appellant respectfully requests that the Board reverse the decision of the Examiner to reject claims 1, 3-10, 13-19 and 21-25 under 35 U.S.C. §103(a), and remand the application to the Examiner for withdrawal of the above-noted rejections.

Respectfully submitted,
D. ANDREEV et al.



Andrew M. Calderon
Reg. No. 38,093

December 9, 2008
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
703-716-1191

Attachments: Claims Appendix,
Evidence Appendix, and
Related Proceedings Appendix

VIII CLAIMS ON APPEAL

1. A method for authentication in a network, the method comprising:

creating a credential string on a portal server, the credential string being an encrypted hash of a session ID;

sending a UserID associated with the session ID and the credential string to a software application from the portal server, while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server;

receiving a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, the confirmation request including the credential string; and

sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID.

3. The method of claim 1, wherein the encrypted hash of the session ID is a derivate of the session ID.

4. The method of claim 1, further comprising the steps of:

performing a lightweight directory access protocol (LDAP) lookup using the UserID; and

if the LDAP lookup confirms the UserID and the response validates the credential string, returning a successful authentication reply to the software application for establishing a session associated with the session ID, otherwise sending an unsuccessful authentication reply to the software application.

5. The method of claim 1, wherein the sending of a UserID and the credential string avoids at least one of sending a user's password outside of a portal server and storing the password in persistent memory.

6. The method of claim 1, further comprising the steps of:

sending the UserID associated with the session ID and the credential string to a software application proxy;

checking whether the session ID and the credential string have been previously received within a predetermined time period; and

if affirmative, initiating a security breach procedure.

7. The method of claim 6, wherein the security breach procedure causes the termination of any session associated with the UserID.

8. The method of claim 1, wherein the receiving step and sending a response step is performed by an authentication proxy.

9. A method for authenticating a user request for a software application, the method comprising:

receiving a UserID and a credential string at an authentication proxy server, the credential string being an encrypted hash of a session ID, which is created at a portal;

sending a confirmation request from the authentication proxy to the portal while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal, the confirmation request includes the credential string;

receiving a response at the authentication proxy for the confirmation request while maintaining the user password on the portal such that the user password is not required to authenticate the User ID; and

validating the UserID using a light weight directory access protocol (LDAP) lookup request and the response.

10. The method of claim 9, further comprising providing a confirmation to the software application if the response is affirmative and the UserID is authenticated by the LDAP lookup.

13. The method of claim 10, further comprising validating the confirmation request by assuring that the credential string has been received only once for confirmation at the portal, otherwise, if presented more than once, performing at least one of initiating a security breach procedure and notifying a software application proxy.

14. The method of claim 9, further comprising receiving the UserID and the user password during a logon to the portal, wherein the UserID is validated in the validating step and the user password is maintained at the portal and used to process the confirmation request.

15. A system for authenticating a session stored on a computer readable storage medium, comprising computer readable program code, comprising:

an authentication proxy which receives requests to authenticate a UserID and a credential string, the credential string being an encrypted hash of a session ID and created on a portal; and

a credential string validation component which receives requests to validate the credential string while maintaining a user password on the portal such that the user password is not required to validate the credential string,

wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period while maintaining the user password on the portal and avoiding exposing the user password to network resources beyond the portal.

16. The system of claim 15, wherein the authentication proxy performs lightweight directory access protocol (LDAP) lookups using the UserID and sends the credential string to the credential string validation component and receives a validation reply.

17. The system of claim 16, wherein the authentication proxy sends an affirmative authentication reply to a software application when both the LDAP lookup is successful and the validation reply indicates a valid credential string.

18. The system of claim 17, wherein the authentication proxy receives the UserID and credential string from a software application.

19. The system of claim 15, further comprising a software application proxy which receives the UserID and the credential string and detects whether the UserID and the credential string have been previously received within a predetermined time period.

21. The system of claim 15, further comprising:

a lightweight directory access protocol (LDAP) directory for authenticating the UserIDs and which is accessible by the authentication proxy; and

a software application proxy for intercepting the UserID and the credential string sent by the portal for monitoring duplicate occurrences of the UserID and the credential string.

22. A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product including at least one program code to:

create a credential string on a portal server, the credential string being an encrypted hash of a session ID;

send a UserID associated with the session ID and the credential string to a software application from the portal server, while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server;

receive a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID, the confirmation request including the credential string; and

send a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID.

23. The system of claim 15, wherein the UserID and the credential string are sent to a software application when the predetermined time period has elapsed.

24. The system of claim 23, wherein a network security breach is initiated when a second request to validate the credential string occurs within the predetermined time period of a first request to validate the credential string.

25. The system of claim 24, wherein the portal is configured to accept a logon by a user and create the credential string from an associated session ID.

IX EVIDENCE APPENDIX

This section lists evidence submitted pursuant to 37 C.F.R. §§1.130, 1.131, or 1.132, or any other evidence entered by the Examiner and relied upon by Appellants in this appeal, and provides for each piece of evidence a brief statement setting forth where in the record that evidence was entered by the Examiner. Copies of each piece of evidence are provided as required by 37 C.F.R. §41.37(c)(ix).

NO.	EVIDENCE	BRIEF STATEMENT SETTING FORTH WHERE IN THE RECORD THE EVIDENCE WAS ENTERED BY THE EXAMINER
1	N/A	N/A

X RELATED PROCEEDINGS APPENDIX

Pursuant to 37 C.F.R. §41.37(c)(x), copies of the following decisions rendered by a court of the Board in any proceeding identified above under 37 C.F.R. §41.37(c)(1)(ii) are enclosed herewith.

NO.	TYPE OF PROCEEDING	REFERENCE NO.	DATE
1	N/A	N/A	N/A